



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/042,262

01/11/2002

Jun Kamada

826.1783

6257

21171 7590 01/25/2008  
STAAS & HALSEY LLP  
SUITE 700  
1201 NEW YORK AVENUE, N.W.  
WASHINGTON, DC 20005

EXAMINER

AUGUSTIN, EVENS J

ART UNIT

PAPER NUMBER

3621

MAIL DATE

DELIVERY MODE

01/25/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/042,262	KAMADA ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	EVENS J. AUGUSTIN	3621	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 01 November 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |  |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)<br>2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)<br>3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____. | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____.<br>5) <input type="checkbox"/> Notice of Informal Patent Application<br>6) <input type="checkbox"/> Other: _____. |
|---|--|

## **DETAILED ACTION**

### **Acknowledgement**

1. Request for Continued Examination under 37 CFR1.114, filed on 11/01/2007, has been acknowledged. Claims 1-22 are pending. The USPTO has considered applicant's arguments/remarks, however, the prior art from the previous office action is maintained because of any patentable distinction that may exist between and current and previous claim language is still unpatentable over the prior art.

### ***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requires of this title.

3. Claim 22 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.
4. As per claim22, the preambles recite, "executing encrypted codes", however, do not recite that the computer program is encoded or recorded on a physical medium readable by a computer. Thus, the claims are directed to functionally descriptive material that is not functionally or structurally interrelated to the medium. Data structures not claimed as embodied in computer readable media (defined as "a collective word for the physical material, such as paper, disk, and tape, used for storing computer-based information", Microsoft Press, Computer Dictionary, Second Edition, © 1994) are descriptive material per se and are not statutory because they are neither physical "things" nor statutory processes.

Such claimed data structures do not define any structural and functional interrelationships between the data structure. See MPEP 2106(IV)(B)(1)(a).

***Claim Rejections - 35 USC § 112 2<sup>nd</sup> Paragraph***

5. The term "normal task" in claims 1-22 is a relative term which renders the claim indefinite.

The term "normal task" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Normal is a relative term. What could be normal for one entity may not be for another. The specification has not established the normalcy, relative to what or whom.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter (US 6427140), in view of Bennett (US 5579520).

1. As per claims 1-22, Ginter et al. discloses an invention that relates to computer-based and other electronic appliance-based technologies that help to ensure that information is accessed and/or otherwise used only in authorized ways, and maintains the integrity, availability, and/or

confidentiality of such information and processes related to such use computer system that relates to development architecture frameworks, and more particularly to managing an environment of a development framework. The invention comprises of the following:

- A. An environment for electronic information owners, distributors, and users; financial clearinghouses; and usage information analyzers and resellers (column 3, lines 45-48)
- B. Multiprocessing system with multiprocessors (column 73, lines 38-40), in which content/software/program/code is encrypted through the components of the multiprocessor system (column 72, lines 31-67, column 73, lines 24-33)
- C. Ginter et al. teaches Memory Management Unit that provides hardware support for memory management and virtual memory management functions. It may also provide heightened security by enforcing hardware compartmentalization/allocation of the secure execution space (e.g., to prevent a less trusted task from modifying a more trusted task) (col. 69, lines 10-15). Basically, Ginter et al. compartmentalizes/separates the execution of secured/trusted/encrypted from the less trusted/unsecured/unencrypted/normal tasks. Additionally, Ginter et al. teach the aspect of allocating task or task manager (column 83, line 36, column 88, lines 51-67). The prior art by Ginter et al. has self-contained computing and processing environments that may include their own operating system kernel including code and data processing resources (column 79, lines 34-37). A kernel manages the basic hardware resources of electronic appliance, and controls the basic tasking provided by the operating system (col. 88, lines 51-53). It also manages allocation, deallocation, sharing and/or use of memory (col. 88, lines 63-65). The environment can recognize

(differentiate or discriminate), process and store secure and non-secure data (col. 80, lines 20-67) (“**a secure memory storing an encrypted code of a secure task and verifying information for verification of validity of the encrypted code**”) (“**a secure processor executing the encrypted code when the validity of the encrypted code is verified according to the verifying information**”) (“**a normal memory storing a code of a normal task; a normal processor executing the code of the normal task**”)

- D. The Examiner takes official notice that the aspect of using a normal memory for normal tasks and a secure memory for secure tasks (memory allocation) is common knowledge in the art (See US 5734822, col. 15, lines 15-25 -- US 6081876 col. 2, lines 8-15 –US 651162, col. 10, lines 53-67, col. 11, lines 1-8) (“**a secure processor executing the encrypted code when the validity of the encrypted code is verified according to the verifying information**”) (“**a normal memory storing a code of a normal task; a normal processor executing the code of the normal task**”)
- E. The environment can recognize (differentiate or discriminate), process and store secure and non-secure data (col. 80, lines 20-67). It also manages allocation, deallocation, sharing and/or use of memory (col. 88, lines 63-65)- During the reply filed on 08 January 2007, applicant admitted that task allocation necessarily has the aspect discriminating (inherent). Applicant states - *the specification clearly states that the secure task management and the secure memory management allocate secure tasks and unsecured tasks. Therefore, the encrypted codes of the secure tasks are stored in the secure memory, and the codes of the unsecured tasks are stored in the*

*normal memory. As allocation necessarily involves discriminating (otherwise, a determination cannot be made as to what tasks should be allocated to what memory), Applicants respectfully submit that the claim term discriminating is fully supported by the specification.* Therefore, “allocating” and “discriminating” will be used interchangeably- (**"discriminating between the secure task and the normal task"**)

- F. Memories stores encrypted and unprotected content (column 21, lines 22-37) (**"storing the encrypted code of the secure task"**)
- G. Verifying information by enforcing hardware compartmentalization/allocation of the secure execution space (e.g., preventing/not allowing a less trusted task from modifying a more trusted task) (col. 69, lines 10-15) (**"verifying information for verification of validity of the encrypted code in a secure memory"**); (**"allowing the secure processor to execute the encrypted code when the validity of the encrypted code is verified according to the verifying information"**)
- H. Content/software/program/code being stored in units of physical allocation memory (bytes) (column 68, line 51) and verified through the components of the multiprocessor system (column 125, lines 60-67) (**"secure memory stores the encrypted code in units of physical memory allocation, stores the verifying information for the encrypted code in the units, and verifies the encrypted code in the units according to the verifying information, and the secure processor fetches, decrypts, and executes an encrypted instruction included in an encrypted code whose validity has been verified"**)

- I. The system also uses digital signature to authenticate the communication of content (column 22, lines 5-10)
- J. Employing a plurality of encryption keys (column 21, lines 65-67, column 22, lines 1-10, column 49, lines 1-59), in an non-volatile memory (column 49, lines 9-12) (“**a plurality of decryption keys, and decrypts the encrypted instruction using a specified decryption key in the plurality of decryption keys**”)
- K. The aspects of using session keys (column 220, lines 20-21) (“**secure memory and said secure processor share a session key after mutual authentication**”)
- L. System uses secure hardware (including drives) with a secure/trusted architecture (column 13, lines 5-25) (“**a secure drive further encrypting the encrypted code using a unique key, and storing the encrypted code, wherein said secure drive and said secure memory share a session key after mutual authentication, said secure drive decrypts the encrypted code using the unique key at a read instruction from said controller, encrypts the code using the session key, and transfers the code to said secure memory**”)
- M. The storing of secure and non-secure information can be stored in a single memory chip or overlapping each other (par. 63, lines 40-43) (“**at least parts of said secure memory and said normal memory overlap each other**”)
- N. The system uses a memory management unit to manage the execution space (column 69, lines 9-42) (“**secure processor fixes at least a part of a logical circuit for executing an encrypted code in a circuit state in a non-volatile manner using the encrypted code.**”)



- O. System teaches Electrically Erasable Programmable Read Only (EEPROM) (column 70, lines 66-67, column 71, lines 1-5) (**“said secure processor erases a previous circuit state of the logical circuit, and newly overwrites the state.”**)
- P. Circuitry designed to "zeroize" memory may be included as an aspect of self-destruct processes (column 64, lines 30-31)
8. Ginter did not explicitly describe a method/system in which a code is generated by assigning a signature in units of a page. However, Bennet describes an invention in which loads information into system memory from disk in fixed-length blocks or "pages" (generally ranging from 4K, for example, to up to 64K or more (C6, L34-36). This is also consistent with Microsoft Computer Dictionary's description of Paging as being: "n. A technique for implementing virtual memory. The virtual address space is divided into a number of fixed-size blocks called pages, each of which can be mapped onto any of the physical addresses available on the system. Special memory management hardware (MMU or PMMU) performs the address translation from virtual addresses to physical addresses".
9. Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to construct a system that would employ a method/system in which a code is generated by assigning a signature in units of a page. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to do so because it would allow hardware units to perform tasks related to accessing and managing memory used by different applications or by virtual-memory operating systems.

***Conclusion***

10. *Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that if the applicant is preparing to respond, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.*
11. In determining patentability of an invention over the prior art, the USPTO has considered all claimed limitations, and interpreted as broadly as their terms reasonably allow. Additionally, all words in the claims have been considered in judging the patentability of the claims against the prior art.
12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Evens Augustin whose telephone number is 571-272-6860. The examiner can normally be reached on Monday thru Friday 8 to 5 pm.
13. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on 571-272-6779.

***/Evens J. Augustin/***

Art Unit: 3621

Evans J. Augustin

January 26, 2008

Art Unit 3621